



Baker&Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

David B. Sherman
direct dial: 215.564.8380
dshe@bakerlaw.com

June 23, 2022

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Brian E. Frosh
Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Attorney General Frosh:

We are writing on behalf of our client, Great Smoky Mountains Association (“GSMA”), to notify you of a security incident.

GSMA recently completed an investigation into suspicious activity on its e-commerce platform that was identified on December 18, 2021. Upon learning of the incident, GSMA promptly took steps to secure its network and commenced an investigation. Through the investigation, GSMA determined that an unknown party added unauthorized code to a portion of its e-commerce website. The code gathered and stored payment card information that was manually submitted by purchasers on GSMA’s e-commerce website between May 21, 2021 and December 18, 2021. GSMA reviewed the transactions on its website during the above timeframe. This review was completed on March 17, 2022. GSMA then conducted a subsequent investigation to locate contact information for the involved individuals to mail notification letters. The information included the name, payment card number, expiration date, and card verification code (“CVV”) of 39 Maryland residents.

On June 23, 2022, GSMA is providing written notice via United States Postal Service mail to the Maryland residents whose information may have been involved in accordance with Md. Code

June 23, 2022

Page 2

Ann., Com. Law § 14-3504. A copy of the notification letter is enclosed.¹ GSMA is encouraging all notice recipients to remain vigilant by reviewing their financial accounts for unauthorized activity. GSMA is also providing a toll-free phone number for notice recipients to call for further information about the incident.

GSMA remains committed to protecting the confidentiality and security of information it maintains. To help prevent something like this from happening again, GSMA is continuing to review and enhance its existing security protocols and practices, including implementation of additional electronic security features.

Please do not hesitate to contact me if you have any questions regarding this incident.

Sincerely,

A handwritten signature in dark ink, appearing to read "David B. Sherman", with a stylized flourish at the end.

David B. Sherman
Partner

Enclosure

¹ This report does not waive GSMA's objection that Maryland lacks personal jurisdiction over it related to any claims that may arise from this incident.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

Great Smoky Mountains Association ("GSMA") values the relationship we have with our customers and understands the importance of protecting your information. We are writing to inform you that we identified and addressed a security incident which involved your payment card information. This notice explains the incident, measures that have been taken, and some steps you may consider taking in response.

What Happened? We concluded an investigation into a data security incident that was identified on December 18, 2021. Upon learning of the incident, we promptly took steps to secure our network, commenced an investigation, and a cybersecurity firm was engaged to assist us. Our investigation found evidence that an unknown party added an unauthorized code to a portion of our e-commerce platform. The code gathered and stored payment card information that was manually submitted by customers during the checkout process on our website between the dates of May 21, 2021 and December 18, 2021. We reviewed the transactions which took place on our website during the above timeframe, to determine what information may have been involved in this incident. This review was completed on March 17, 2022. We then conducted research to gather information to send notice to individuals whose information was involved in this incident.

What Information Was Involved? Our investigation determined that the information collected included your name, address, payment card number, expiration date and card security code.

What We Are Doing: GSMA takes this matter very seriously and we are continuing to enhance the security on our e-commerce platform to help prevent a similar incident from occurring in the future. We are also in the process of transitioning to a new checkout process with additional security features.

What You Can Do: We encourage you to closely review your payment card statements for any unauthorized charges. We recommend that you immediately report any such charges to the bank that issued your card. If reported timely, payment card network rules generally provide that cardholders are not responsible for unauthorized charges. Information on additional steps you can take can be found on the following pages.

For More Information: We regret any inconvenience or concern this may cause. If you have any questions, please contact us at 844-686-2099, Monday through Friday, between 9:00 A.M. – 9:00 P.M., Eastern Time (except for on major U.S. holidays).

Sincerely,

Laurel Rematore
Chief Executive Officer

P.O. BOX 130, GATLINBURG, TN 37738
PH: 865.436.7318 • TOLL-FREE 888.898.9102
SMOKIESINFORMATION.ORG

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your credit or debit card statements, financial account statements, and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

District of Columbia: You may contact Atlantic Coast Brands via mail at 100 Town Square Place, 6th Floor, Jersey City, NJ

07310 and via phone at 888-805-5249. You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Maryland: You may contact Atlantic Coast Brands via mail at 100 Town Square Place, 6th Floor, Jersey City, NJ 07310. You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact Atlantic Coast Brands via mail at 100 Town Square Place, 6th Floor, Jersey City, NJ 07310 and via phone at 888-805-5249. You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves <<RI Count>> individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.